AXIS A9210 Network I/O Relay Module

User manual

Get started

Find the device on the network

To find Axis devices on the network and assign them IP addresses in Windows®, use AXIS IP Utility or AXIS Device Manager. Both applications are free and can be downloaded from *axis.com/support*.

For more information about how to find and assign IP addresses, go to *How to assign an IP address and access your device*.

Browser support

You can use the device with the following browsers:

	Chrome™	Edge™	Firefox®	Safari®
Windows®	✓	✓	*	*
macOS®	✓	✓	*	*
Linux®	✓	✓	*	*
Other operating systems	*	*	*	*

✓: Recommended

*: Supported with limitations

Open the device's web interface

1. Open a browser and type the IP address or host name of the Axis device.
   If you don't know the IP address, use AXIS IP Utility or AXIS Device Manager to find the device on the network.
2. Type the username and password. If you access the device for the first time, you must create an administrator account. See *Create an administrator account, on page 2*.

For descriptions of all features and settings in the web interface of devices with AXIS OS, see *AXIS OS web interface help*.

Create an administrator account

The first time you log in to your device, you must create an administrator account.

1. Enter a username.
2. Enter a password. See *Secure passwords, on page 3*.
3. Re-enter the password.
4. Accept the license agreement.
5. Click **Add account**.

Important

The device has no default account. If you lose the password for your administrator account, you must reset the device. See *Reset to factory default settings, on page 15*.

Secure passwords

Important

Use HTTPS (which is enabled by default) to set your password or other sensitive configurations over the network. HTTPS enables secure and encrypted network connections, thereby protecting sensitive data, such as passwords.

The device password is the primary protection for your data and services. Axis devices do not impose a password policy as they may be used in various types of installations.

To protect your data we strongly recommend that you:

- Use a password with at least 8 characters, preferably created by a password generator.
- Don't expose the password.
- Change the password at a recurring interval, at least once a year.

Make sure that no one has tampered with the device software

To make sure that the device has its original AXIS OS, or to take full control of the device after a security attack:

1. Reset to factory default settings. See *Reset to factory default settings, on page 15*.
   After the reset, secure boot guarantees the state of the device.
2. Configure and install the device.

Web interface overview

This video gives you an overview of the device's web interface.



Axis device web interface

Configure your device

Configure an I/O port

1. Go to **Device > I/Os and relays > AXIS A9210 > I/Os**.
2. Click to expand the I/O port settings.
3. Rename the port.
4. Configure the normal state. Click for open circuit, or for closed circuit.
5. To configure the I/O port as input:
   5.1. Under **Direction**, click .
   5.2. To monitor the input state, turn on **Supervised**. See *Supervised inputs, on page 13*.

Note

In APIs, the supervised I/O ports work differently from the supervised input ports. For more information, go to the *VAPIX® Library*.

6. To configure the I/O port as output:
   6.1. Under **Direction**, click .
   6.2. To view the URLs to activate and deactivate connected devices, go to **Toggle port URL**.

Configure a relay

1. Go to **Device > I/Os and relays > AXIS A9210 > Relays**.
2. Click to expand the relay settings.
3. Turn on **Relay**.
4. Rename the relay.
5. To view the URLs to activate and deactivate the relay, go to **Toggle port URL**.

Set up rules for events

To learn more, see *Get started with rules for events*.

Trigger an action

1. Go to **System > Events** and add a rule. The rule defines when the device will perform certain actions. You can set up rules as scheduled, recurring, or manually triggered.
2. Enter a **Name**.
3. Select the **Condition** that must be met to trigger the action. If you specify more than one condition for the rule, all of the conditions must be met to trigger the action.
4. Select which **Action** to perform when the conditions are met.

Note

- If you make changes to an active rule, the rule must be turned on again for the changes to take effect.

The web interface

To read about all the features and settings available in the web interface of devices with AXIS OS, go to *AXIS OS web interface help*.

Learn more

Analytics and apps

With analytics and apps you can get more out of your Axis device. AXIS Camera Application Platform (ACAP) is an open platform that makes it possible for third parties to develop analytics and other apps for Axis devices. Apps can be preinstalled on the device, available for download for free, or for a license fee.

To find the user manuals for Axis analytics and apps, go to *help.axis.com*.

AXIS Door Monitoring

This application monitors the door status, showing whether the door is open or closed, and if it stays open for too long. For example, use this application on a fire safety door that doesn't require a lock but where you need to know if it is open.

A regular door has a door position sensor, REX, along with locks and readers, which requires a door controller.

A monitoring door requires only a door position sensor and REX, and can be monitored using a network I/O relay module. Each network I/O relay module can connect up to five monitoring doors.

Limitations

The application is only available on AXIS A9210. REX can only be connected to I/O 1 and I/O 2, not possible to configure REX on I 3, I 4, or I 5.

AXIS Monitoring Door Configuration

Name	Description
Door	The number of the door.
DPS input	The DPS input for the door.
REX input	The REX input for the door.
Door open too long time (sec)	The number of seconds the door is allowed to stay open.
Access time (sec)	The number of seconds the door shall remain unlocked after access has been granted.
State	The state of the door.

Cybersecurity

For product-specific information about cybersecurity, see the product's datasheet at axis.com.

For in-depth information about cybersecurity in AXIS OS, read the *AXIS OS Hardening guide*.

Axis Edge Vault

Axis Edge Vault provides a hardware-based cybersecurity platform that safeguards the Axis device. It offers features to guarantee the device's identity and integrity and to protect your sensitive information from unauthorized access. It builds on a strong foundation of cryptographic computing modules (secure element and TPM) and SoC security (TEE and secure boot), combined with expertise in edge device security.

Signed OS

Signed OS is implemented by the software vendor signing the AXIS OS image with a private key. When the signature is attached to the operating system, the device will validate the software before installing it. If the device detects that the integrity of the software is compromised, the AXIS OS upgrade will be rejected.

Secure boot

Secure boot is a boot process that consists of an unbroken chain of cryptographically validated software, starting in immutable memory (boot ROM). Being based on the use of signed OS, secure boot ensures that a device can boot only with authorized software.

Secure keystore

A tamper-protected environment for the protection of private keys and secure execution of cryptographic operations. It prevents unauthorized access and malicious extraction in the event of a security breach. Depending on security requirements, an Axis device can have either one or multiple hardware-based cryptographic computing modules, which provide a hardware-protected secure keystore. Depending on security requirements, an Axis device can have either one or multiple hardware-based cryptographic computing modules, like a TPM 2.0 (Trusted Platform Module) or a secure element, and/or a TEE (Trusted Execution Environment), which provide a hardware-protected secure keystore. Furthermore, selected Axis products feature a FIPS 140-2 Level 2-certified secure keystore.

Axis device ID

Being able to verify the origin of the device is key to establishing trust in the device identity. During production, devices with Axis Edge Vault are assigned a unique, factory-provisioned, and IEEE 802.1AR-compliant Axis device ID certificate. This works like a passport to prove the origin of the device. The device ID is securely and permanently stored in the secure keystore as a certificate signed by Axis root certificate. The device ID can be leveraged by the customer's IT infrastructure for automated secure device onboarding and secure device identification

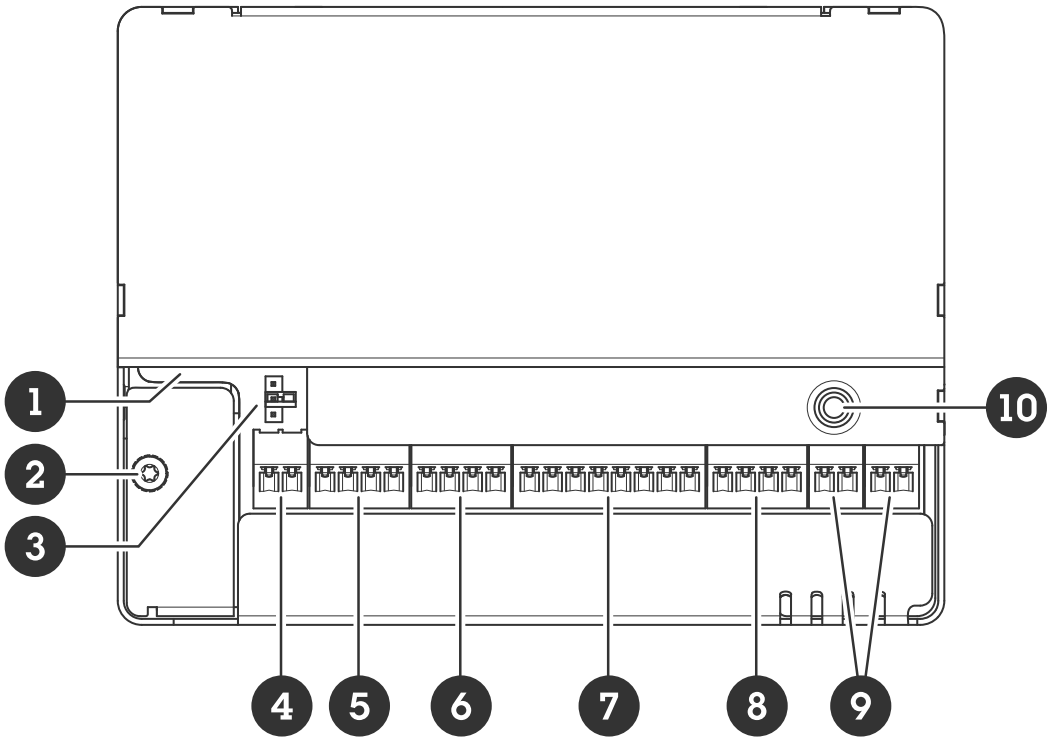
Encrypted file system

The secure keystore prevents the malicious exfiltration of information and prevents configuration tampering by enforcing strong encryption upon the file system. This ensures no data stored in the file system can be extracted or tampered with when the device is not in use, unauthenticated access to the device is achieved and/or the Axis device is stolen. During the secure boot process, the read-write filesystem is decrypted and can be mounted and used by the Axis device.

To learn more about the cybersecurity features in Axis devices, go to *axis.com/learning/white-papers* and search for cybersecurity.

Specifications

Product overview



1 *Network connector*
2 *Grounding position*
3 *Relay jumper*
4 *Power connector*
5 *Relay connector*
6 *Input 1 connector*
7 *RS485 and I/O connector*
8 *I/O connector*
9 *Input 2 connector*
10 *Control button*

LED indicators

LED	Color	Indication
Status	Green	Steady green for normal operation.
	Amber	Steady during startup and when restoring settings.
	Red	Slow flash for failed upgrade.
Network	Green	Steady for connection to a 100 MBit/s network. Flashes for network activity.
	Amber	Steady for connection to a 10 MBit/s network. Flashes for network activity.
	Unlit	No network connection.
Power	Green	Normal operation.

	Amber	Flashes green/amber during firmware upgrade.
Relay	Green	Relay active.[1]
	Unlit	Relay inactive.

Buttons

Control button

The control button is used for:

- Resetting the product to factory default settings. See *Reset to factory default settings, on page 15*.
- Connecting to a one-click cloud connection (O3C) service over the internet. To connect, press and release the button, then wait for the status LED to flash green three times.

Connectors

Network connector

RJ45 Ethernet connector with Power over Ethernet Plus (PoE+).

UL: Power over Ethernet (PoE) shall be over Ethernet IEEE 802.3af/802.3at Type 1 Class 3 or Power over Ethernet Plus (PoE+) IEEE 802.3at Type 2 Class 4 power limited injector that provides 44–57 V DC, 15.4 W / 30 W. Power over Ethernet (PoE) has been evaluated by UL with AXIS T8133 Midspan 30 W 1-port.

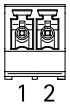
Power priority

This device can be powered by either PoE or DC input. See *Network connector, on page 9* and *Power connector, on page 9*.

- When PoE and DC are both connected before the device is powered, PoE is used for powering.
- PoE and DC are both connected and PoE is currently powering. When PoE is lost, the device uses DC for powering without restart.
- PoE and DC are both connected and DC is currently powering. When DC is lost, the device restarts and uses PoE for powering.
- When DC is used during startup and PoE is connected after the device has started, DC is used for powering.
- When PoE is used during startup and DC is connected after the device has started, PoE is used for powering.

Power connector

2-pin terminal block for DC power input. Use a Safety Extra Low Voltage (SELV) compliant limited power source (LPS) with either a rated output power limited to ≤100 W or a rated output current limited to ≤5 A.



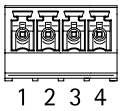
1. *Relay is active when COM is connected to NO.*

Function	Pin	Notes	Specifications
DC ground (GND)	1		0 V DC
DC input	2	For powering the device when not using Power over Ethernet. Note: This pin can only be used as power in.	12 V DC, max 36 W

UL: DC power to be supplied by a UL 603 listed power supply, depending on application, with appropriate ratings.

Relay connector

One 4-pin terminal block for form C relays that can be used, for example, to control a lock or an interface to a gate. If used with an inductive load, for example a lock, connect a diode in parallel with the load to protect against voltage transients.



Function	Pin	Notes	Specifications
DC ground (GND)	1		0 V DC
NO	2	Normally open. For connecting relay devices. Connect a fail-secure lock between NO and DC ground. The two relay pins are galvanically separated from the rest of the circuitry if the jumpers are not used.	Max current = 2 A Max voltage = 30 V DC
COM	3	Common	
NC	4	Normally closed. For connecting relay devices. Connect a fail-safe lock between NC and DC ground. The two relay pins are galvanically separated from the rest of the circuitry if the jumpers are not used.	

Relay power jumper

When the relay power jumper is fitted, it connects 12 V DC or 24 V DC to the relay COM pin.

It can be used to connect a lock between the GND and NO, or GND and NC pins.

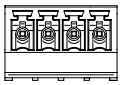
Power source	Max power at 12 V DC	Max power at 24 V DC
DC IN	2 000 mA	1 000 mA

PoE	350 mA	150 mA
PoE+	1100 mA	500 mA

Input 1 connector

One 4-pin terminal block for input.

It supports supervision with end of line resistors. If the connection is interrupted, an alarm is triggered. To use supervised inputs, install end of line resistors. Use the connection diagram for supervised inputs. See *Supervised inputs, on page 13*.



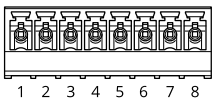
Function	Pin	Notes	Specifications
DC ground	1, 3		0 V DC
Input	2, 4	Digital input or supervised input — Connect to pin 1 or 3 respectively to activate, or leave floating (unconnected) to deactivate.	0 to max 30 V DC

Important

The qualified cable length is up to 200 m (656 ft) if the following cable requirement is met: AWG 24.

RS485 and I/O connector

One 8-pin terminal block including 4-pin RS485 and 4-pin I/O.



RS485

Function	Pin	Note	Specifications
DC ground (GND)	1		0 V DC
DC output (+12 V)	2	Supplies power to auxiliary devices, for example, Modbus sensors.	12 V DC, max 200 mA
A	3		
B	4		

I/O

Function	Pin	Note	Specifications
Digital output	5	If used with an inductive load, for example a relay, connect a diode in parallel with the load to protect against voltage transients.	0 to max 30 V DC, open drain, 100 mA

Digital output	6	If used with an inductive load, for example a relay, connect a diode in parallel with the load to protect against voltage transients.	0 to max 30 V DC, open drain, 100 mA
Input	7	Digital input or supervised input — Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 30 V DC
Digital output	8	If used with an inductive load, for example a relay, connect a diode in parallel with the load to protect against voltage transients.	0 to max 30 V DC, open drain, 100 mA

Important

- The qualified cable length for RS485 is up to 1000 m (3281 ft) if the following cable requirements are met: 1 twisted pair with shield, AWG 24, 120 ohm impedance.
- The qualified cable length for I/O is up to 200 m (656 ft).

I/O connector

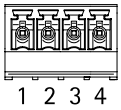
Use the auxiliary connector with external devices in combination with, for example, motion detection, event triggering, and alarm notifications. In addition to the 0 V DC reference point and power (DC output), the auxiliary connector provides the interface to:

Digital input – For connecting devices that can toggle between an open and closed circuit, for example PIR sensors, door/window contacts, and glass break detectors.

Supervised input – Enables possibility to detect tampering on a digital input.

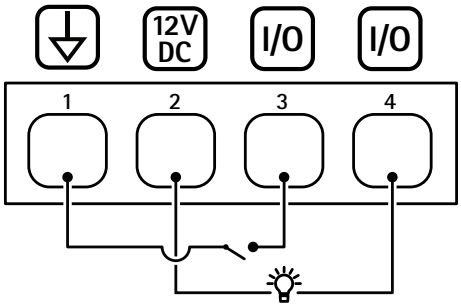
Digital output – For connecting external devices such as relays and LEDs. Connected devices can be activated by the VAPIX® Application Programming Interface or from the product's webpage.

4-pin terminal block



Function	Pin	Notes	Specifications
DC ground	1		0 V DC
DC output	2	Can be used to power auxiliary equipment. Note: This pin can only be used as power out.	12 V DC Max load = 50 mA in total
Configurable (Input or Output)	3–4	Digital input or supervised input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate. To use supervised input, install end-of-line resistors. See connection diagram for information about how to connect the resistors.	0 to max 30 V DC

		Digital output – Internally connected to pin 1 (DC ground) when active, and floating (unconnected) when inactive. If used with an inductive load, e.g., a relay, connect a diode in parallel with the load, to protect against voltage transients. I/Os are capable of driving 12 V DC, 50 mA (combined max) external load, if internal 12 V DC output (pin 2) is used. In the case of using open drain connections in combination with an external power supply, then the I/Os can manage DC supply of 0–30 V DC, 100 mA each.	0 to max 30 V DC, open drain, 100 mA

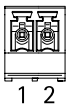


1 DC ground
2 DC output 12 V
3 I/O configured as input
4 I/O configured as output

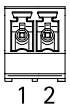
Input 2 connector

Two 2-pin terminal blocks for external devices, for example glass break or fire detectors.

UL: The connector has not been evaluated by UL for burglar or fire alarm use.



Function	Pin	Notes	Specifications
DC ground	1		0 V DC
Input	2	Digital input or supervised input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 30 V DC



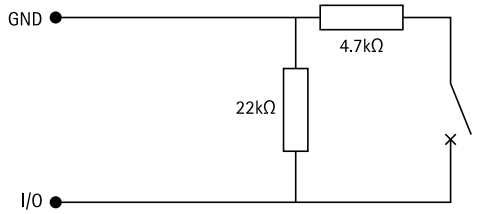
Function	Pin	Notes	Specifications
DC ground	1		0 V DC
Input	2	Digital input or supervised input – Connect to pin 1 to activate, or leave floating (unconnected) to deactivate.	0 to max 30 V DC

Supervised inputs

To use supervised inputs, install end of line resistors according to the diagram below.

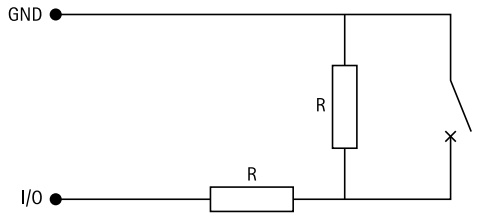
Parallel first connection

The resistor values must be 4.7 kΩ and 22 kΩ.



Serial first connection

The resistor values must be the same and possible values are 1 kΩ, 2.2 kΩ, 4.7 kΩ and 10 kΩ, 1%, ¼ watt standard.



Note

It is recommended to use twisted and shielded cables. Connect shielding to 0 V DC.

Status	Description
Open	The supervised switch is in open mode.
Closed	The supervised switch is in closed mode.
Short	The I/O or Input 1-5 cable is short circuit to GND.
Cut	The I/O or Input 1-5 cable is cut and left open with no current path to GND.

Troubleshooting

Reset to factory default settings

Important

Reset to factory default should be used with caution. A reset to factory default resets all settings, including the IP address, to the factory default values.

To reset the product to the factory default settings:

1. Disconnect power from the product.
2. Press and hold the control button while reconnecting power. See *Product overview, on page 8*.
3. Keep the control button pressed for 25 seconds until the status LED indicator turns amber for the second time.
4. Release the control button. The process is complete when the status LED indicator turns green. If no DHCP server is available on the network, the device IP address will default to one of the following:
   - **Devices with AXIS OS 12.0 and later:** Obtained from the link-local address subnet (169.254.0.0/16)
   - **Devices with AXIS OS 11.11 and earlier:** 192.168.0.90/24
5. Use the installation and management software tools, assign an IP address, set the password, and access the product.

You can also reset parameters to factory default through the device's web interface. Go to **Maintenance** > **Factory default** and click **Default**.

AXIS OS options

Axis offers device software management according to either the active track or the long-term support (LTS) tracks. Being on the active track means continuously getting access to all the latest product features, while the LTS tracks provide a fixed platform with periodic releases focused mainly on bug fixes and security updates.

Using AXIS OS from the active track is recommended if you want to access the newest features, or if you use Axis end-to-end system offerings. The LTS tracks are recommended if you use third-party integrations, which are not continuously validated against the latest active track. With LTS, the products can maintain cybersecurity without introducing any significant functional changes or affecting any existing integrations. For more detailed information about Axis device software strategy, go to *axis.com/support/device-software*.

Check the current AXIS OS version

AXIS OS determines the functionality of our devices. When you troubleshoot a problem, we recommend that you to start by checking the current AXIS OS version. The latest version might contain a correction that fixes your particular problem.

To check the current AXIS OS version:

1. Go to the device's web interface > **Status**.
2. Under **Device info**, see the AXIS OS version.

Upgrade AXIS OS

Important

- When you upgrade the device software, your preconfigured and customized settings are saved. Axis Communications AB can't guarantee that the settings are saved, even if the features are available in the new AXIS OS version.
- Starting from AXIS OS 12.6, you must install every LTS version between your device's current version and the target version. For example, if the currently installed device software version is AXIS OS 11.2, you

have to install the LTS version AXIS OS 11.11 before you can upgrade the device to AXIS OS 12.6. For more information, see *AXIS OS Portal: Upgrade path*.

- Make sure the device remains connected to the power source throughout the upgrade process.

Note

- When you upgrade the device with the latest AXIS OS version in the active track, the product receives the latest functionality available. Always read the upgrade instructions and release notes available with each new release before you upgrade. To find the latest AXIS OS version and the release notes, go to *axis.com/support/device-software*.

1. Download the AXIS OS file to your computer, available free of charge at *axis.com/support/device-software*.
2. Log in to the device as an administrator.
3. Go to **Maintenance > AXIS OS upgrade** and click **Upgrade**.

When the upgrade has finished, the product restarts automatically.

Technical problems and possible solutions

Problems upgrading AXIS OS

AXIS OS upgrade failed

If the upgrade fails, the device reloads the previous version. The most common reason is that the wrong AXIS OS file has been uploaded. Check that the name of the AXIS OS file corresponds to your device and try again.

Problems after AXIS OS upgrade

If you experience problems after the upgrade, roll back to the previously installed version from the **Maintenance** page.

Problems setting the IP address

Can't set the IP address

- If the IP address intended for the device and the IP address of the computer used to access the device are located on different subnets, you can't set the IP address. Contact your network administrator to obtain an IP address.
- The IP address could be in use by another device. To check:
  1. Disconnect the Axis device from the network.
  2. In a Command/DOS window, type `ping` and the IP address of the device.
  3. If you receive: `Reply from <IP address>: bytes=32; time=10...` this means that the IP address might already be in use by another device on the network. Obtain a new IP address from the network administrator and reinstall the device.
  4. If you receive: `Request timed out`, this means that the IP address is available for use with the Axis device. Check all cabling and reinstall the device.
- There could be a possible IP address conflict with another device on the same subnet. The static IP address in the Axis device is used before the DHCP server sets a dynamic address. This means that if the same default static IP address is also used by another device, there could be problems accessing the device.

Problems accessing the device

Can't log in when accessing the device from a browser

When HTTPS is enabled, make sure that you use the correct protocol (HTTP or HTTPS) when you try to log in. You might need to manually type `http` or `https` in the browser's address field.

If you've lost the password for the root account, you must reset the device to the factory default settings. For instructions, see *Reset to factory default settings, on page 15*.

The IP address has been changed by DHCP

IP addresses obtained from a DHCP server are dynamic and could change. If the IP address has been changed, use AXIS IP Utility or AXIS Device Manager to locate the device on the network. Identify the device using its model or serial number, or by the DNS name (if the name has been configured).

If required, you can assign a static IP address manually. For instructions, go to *axis.com/support*.

Certificate error when using IEEE 802.1X

For authentication to work properly, the date and time settings in the Axis device must be synchronized with an NTP server. Go to **System > Date and time**.

The browser isn't supported

For a list of recommended browsers, see *Browser support, on page 2*.

Can't access the device externally

To access the device externally, we recommend you to use one of the following applications for Windows®:

- AXIS Camera Station Pro: 90-day trial version free of charge, ideal for small to mid-size systems.

For instructions and download, go to *axis.com/vms*.

Problems with MQTT

Can't connect over port 8883 with MQTT over SSL

The firewall blocks traffic that uses port 8883 since it's regarded insecure.

In some cases the server/broker might not provide a specific port for MQTT communication. It might still be possible to use MQTT over a port normally used for HTTP/HTTPS traffic.

- If the server/broker supports WebSocket/WebSocket Secure (WS/WSS), typically on port 443, use this protocol instead. Check with the server/broker provider to see if WS/WSS is supported and which port and basepath to use.
- If the server/broker supports ALPN, the use of MQTT can be negotiated over an open port, such as 443. Check with your server/broker provider to see if ALPN is supported and which ALPN protocol and port to use.

Problems with operating the device

Front heater and wiper aren't working

If the front heater or wiper are not turning on, confirm that the top cover is properly fastened to the bottom of the housing unit.

If you can't find what you're looking for here, try the troubleshooting section at *axis.com/support*.

Contact support

If you need more help, go to *axis.com/support*.

T10202445

2026-02 (M7.2)

© 2023 – 2026 Axis Communications AB